CONTROLLED PROXY SECURE END TO END COMMUNICATION

ABSTRACT OF THE DISCLOSURE

A session key is developed for communication between two end to end users where one or both of the end users do not have the computation capability of carry out all the steps required to generate a secure session key. End user limitations may include lack of computer storage, bandwidth or power supply capability to support the programs necessary for the computation and authentication of the protocol steps. The invention teaches the use of at least one intermediary proxy, which may be network servers or a telephone service providers, and who hold securitiy certificates supporting the use of public and private keys in the transmission of encrypted information. The end users channel their requests through the proxies, who perform the protocol computations and act as trusted intermediaries in transferring the computation results between the end users in establishing a secure session key.